# Release Notes

==========

| | |
|---|---|
| Product: | IBM Security Guardium |
| Release: | v10.6 |
| Version | Guardium v10.0 GPU 600 |
| Completion Date: | 2018-December-11 |
| Revised: | 2019-March-18 |

IBM Security Guardium is designed to help safeguard critical data.

Guardium is a comprehensive data protection platform that enables security teams to automatically analyze sensitive-data environments such as databases, data warehouses, big data platforms, cloud environments, file systems, mainframes, IBM Z®, IBM i platforms, and so on.

Guardium minimizes risk, protects sensitive data from internal and external threats, and seamlessly adapts to IT changes that may impact data security. It ensures the integrity of information in data centers and automates compliance controls like GDPR, HIPAA, SOX, PCI, and others.

Guardium provides a suite of programs organized around components and modules:

- IBM Security Guardium Appliances
- IBM Security Guardium Data Security and Compliance
    - IBM Security Guardium Data Protection
    - IBM Security Guardium Data Activity Monitor
    - IBM Security Guardium Vulnerability Assessment
- IBM Security Guardium for Files
    - IBM Security Standard Activity Monitor for Files
    - IBM Security Advanced Activity Monitor for Files
- IBM Security Guardium Data Protection for NAS
- IBM Security Guardium Data Protection for SharePoint
- IBM Security Guardium Multi-Cloud Data Protection

# Table of Contents

# Guardium 10.6 - Installing and Upgrading

Read through this document before you begin installation.

ISO or GPU:
For Guardium release v10.6, the software is available as an ISO product image from Passport Advantage and as a GPU from Fix Central.

Passport Advantage:
ibm.com/software/howtobuy/passportadvantage/pao_customers.htm
On Passport Advantage (PA), you'll find the Guardium Product Image - ISO file, licenses, product keys, and manuals. You may only download the products that your site is entitled.
If you need assistance finding or downloading a product from the Passport Advantage site, contact the Passport Advantage team at 800-978-2246 (8:00 AM - 8:00 PM EST) or by email paonline@us.ibm.com.

Fix Central:
ibm.com/support/fixcentral
On Fix Central, you'll find Guardium Patch Update files (GPUs), individual patches and the current versions of STAP and GIM.

If you need assistance finding a product on Fix Central, contact Guardium support.

**Upgrading to v10.6**

v10.6 (v10.0 GPU 600) can be installed on any v10.x system regardless of whether it was upgraded from v9.x or built from an earlier v10.x image.

The only dependency is that v10.0 Health Check patch 9997 must be successfully installed before installing the Guardium v10.6 (v10.0 GPU 600). See the section Health Check patch.

v10.6 (v10.0 GPU 600) includes all previous v10.x fix packs, security fixes and sniffer patches.

To help speed up this upgrade, Guardium customers must backup, archive and purge the appliance data as much as possible. During GPU upgrades, the appliance's internal database will shut down. Depending on the size of the database, it might take an extended amount of time to restart. During this time, CLI access will only be available in recovery mode.

In recovery mode, the following CLI message will display:
The internal database on the appliance is currently down and CLI will be working in 'recovery mode'; only a limited set of commands will be available.

**Important:** Do NOT reboot the system during the internal database upgrade.
For real-time details on the system patch installation, use the CLI command `show system patch status`. For v10.6, you can run this command in the CLI recovery mode, but only after a certain point in the v10.0 GPU 600 installation when the CLI command gets added.

**Note for appliances upgrading from v10.1.2 and lower:**
When using the GUI (fileserver method) to upload GPU 600, there is a risk of time out because of the large file size.
Recommendation: Use the CLI command `system patch install`. For more information on this command, see Store system patch install.

**Health Check patch**

The v10.0 Health Check patch 9997 must be successfully installed in the last seven days before installing Guardium v10.6 (v10.0 GPU 600).

If the Health Check patch isn't installed as recommended, GPU 600 will fail with this error message:
`Patch Installation Failed - Latest patch 10.0p9997 required.`

The Health Check file is a compressed file with the file name in this format:
SqlGuard_10.0p9997_HealthCheck_<date>.zip.

Note: Always use the latest and newest version of Health Check patch on Fix Central, even if you have the Health Check patch from earlier GPUs.

**General Notes**

This GPU patch will restart the appliance.

Installation must be scheduled during a "quiet" time on the Guardium appliance to avoid conflicts with other long-running processes such as heavy reports, audit processes, backups and imports.

Purge as much unneeded data as possible for an easier installation process.

If the downloaded package is in .ZIP format, customers are required to extract it outside the Guardium appliance before uploading or installing it.

To avoid aggregator merge issues, install this patch both on a collector and corresponding aggregator appliance.

**Important:** Installation must be across all the appliances: central manager, aggregators, and collectors.

**Installing or upgrading to 10.6 Windows S-TAP**

Fresh install of v10.6 - no reboot required
Upgrading from v9 to v10.6 - no reboot required
Upgrading from v10.0 and build lower than 83909 - reboot is required
Upgrading from v10.1.x (revisions lower than Windows STAP v10.1.22.16) - reboot is required

# New Features and Enhancements

Guardium v10.6 introduces new features and enhancements.

**UI-Based Enhancements**

**Policy builder for data**
The new policy builder simplifies policy management with enhancements like sorting and filtering by properties, exporting CSVs with policy and rule properties, and dedicated collection profile rule types. For more information, see Policies.

**Session-level policies**
Support for session-level policies improves policy processing for rules that fire on session or access level information. It works with both UNIX and Windows S-TAPs. See Session-level Policies.

**Outliers Mining**
New default dashboards to assist investigating outlier findings, support for environments with multiple central managers, a simplified API for enabling and disabling, and an enhanced outlier mining status page. For more information, see Outliers Detection.

**Query-report builder**
The new query-report builder combines the legacy report and query builders into a simplified workflow where each query represents one corresponding report. For more information, see Using the Query-Report Builder.

**Disk and Database Health Analyzer**
In addition to monitoring, Guardium now predicts database sizes and files on disk (/var). When it identifies a database whose size, or files on disk (/var), might potentially reach 50 percent in the next 14 days, it sends alerts. Alerts also appear in the deployment health dashboard of the central manager. See Self-Monitoring.

**Guardium Logins Report:**
The Guardium Logins report now displays the CLI user name, the login date and time, logout date and time and remote host information for both successful and failed logins. The report previously captured only GUI logins. To access this report through the GUI, navigate to Reports > Monitoring of Guardium System > Guardium Logins.

**Cloud Deployment**

**External S-TAP**
Guardium External S-TAP intercepts traffic for cloud and on-premises database services without installing an agent on the database server. This component is available as a Docker image and can be deployed anywhere. For more information about installing and using External S-TAP, see External S-TAP. For the External S-TAP Docker image, go to Docker store External S-TAP.

**GIM**

**GIM Enhancements**
Set up by Client enhancements: GIM group builder and Generate API function. Ability to see installed modules when choosing the client. See Setup by Client.

## Vulnerability Assessment

### Vulnerability Assessment support for multi-threading

Vulnerability assessment support for multi-threading reduces scan time by scheduling and running multiple security assessments in parallel, allowing you to run two concurrent scans for each CPU core. For more information, see Multi-thread Assessment.

## Windows S-TAP

### FAM MS-Office events consolidation

Guardium can filter out the extraneous, irrelevant MS Word, Excel, and PowerPoint file activities from FAM monitoring. See Configuring consolidation of FAM MS Office events.

### Firewall

The Windows parameter, firewall_default_state, has a new state that uses session level policies for decisions, reducing latency and improving performance. See firewall_default_state for Windows S-TAP.

### Pre-kernel Dump Verification

S-TAP now comes packaged with a pre-kernel dump verification utility called System Verification Tool. This tool helps customers determine if their dump settings in the registry are configured correctly so that a kernel dump can be successfully performed. For more information, see Pre-Kernel dump verification utility for Windows S-TAP.

## UNIX S-TAP

### S-TAP Resilience

S-TAP resilience identifies user configuration errors that S-TAP could not validate. The S-TAP remains connected to Guardium appliance even if the user made significant mistakes in the configuration. In this case, the STAP control status will be yellow. Access the Event Log from the S-TAP Control page to view and rectify the errors. See Linux and UNIX systems: Configure S-TAP from the GUI.

### DB2 exit health check script

The DB2 exit health check script gathers information from the DB2 server, used for configuring and troubleshooting the DB2 IEs. See DB2 Exit integration with S-TAP S-TAP is not capturing DB2 exit traffic.

### Exit libraries

When upgrading S-TAP with an exit library to 10.6, the database still requires restart. However, when upgrading v10.6 S-TAP to a higher version, an immediate database restart would no longer be required. See Linux and UNIX systems: Using Exit Libraries.

### Cassandra auditing

Cassandra auditing can log to a file appender. See Linux and UNIX systems: Configure Cassandra auditing to log to a FileAppender.

### Firewall

The UNIX S-TAP parameter, firewall_default_state, has a new state that uses session level policies for decisions, reducing latency and improving performance. See Firewall.

## File Activity Monitor (FAM)

### FAM for GDPR

A new FAM for GDPR accelerator provides policies, discovery and classification, and reports for GDPR readiness. For more information, see FAM Accelerator overview.

### FAM for NAS and SharePoint

FAM adds a new feature to monitor and audit SharePoint servers and network-attached storage devices in the Windows environment. For more information, see File Activity Monitor for NAS and SharePoint.

## CAS (Configuration Auditing System)

### CAS Installer

CAS joins the other Guardium agents on Windows servers with a new .NET installer.
See Installing CAS.

## Additional Enhancements

### Oracle Datasource

Guardium 10.6 supports datasource connections with SSL with server-signed and mutual authentication. SSL connections can be initiated using either the DataDirect or Oracle JDBC driver.

### Guardium Password Enhancements:

Stronger Passwords:
Guardium GUI passwords are now compliant with STIG rule APP3320. Admins can enable strong password compliance using the CLI command `strong_password_enable`. Note: This feature is enforced on local Guardium appliance users only. Admins who have configured LDAP won't see the new behavior changes for strong passwords.

Password Hashing:
User passwords for the Guardium GUI are now hashed with a stronger password hashing algorithm that's compliant with industry standards.

LDAP Authentication:
Guardium now supports LDAP authentication. Customers using LDAP will no longer need to create separate local user IDs. The local user & password will be the LDAP user & LDAP password. Note: Upgrading customers must delete existing local users using the `setguiuser` CLI command.

For more information on passwords, see User Account, Password and Authentication CLI Commands.

### GDPR readiness

Follow these guidelines to configure your Guardium system for GDPR readiness:
GDPR Readiness.

**Discover sensitive data**
The discover sensitive data tool replaces the classification policy builder and classification process builder and adds support for reusing both policies and audit processes. For more information, see Discover Sensitive Data.

**TSM (Tivoli Storage Manager) v7.1.8**
Guardium now supports TSM v7.1.8. To configure TSM Archive or backup, see Configure TSM v7.1.8.

**SAN (Subject Alternative Name) Support:**
SAN support has been added to the CLI commands: `create csr alias`, `create csr external_stap`, `create csr gim` and `create csr gui`. There are ten SAN slots for each CSR generation command. Nine of the SANs are optional and can be added in FQDN (Fully Qualified Domain Name) format. The first SAN slot is reserved for CN- Common Name. For usage information, see Certificate CLI commands.

# Vulnerability Assessment

### 1) MySQL CIS Benchmark

IBM Guardium Vulnerability assessment supports CIS's latest MySQL 5.6 & 5.7 benchmark version 1.0 & 1.1 in v10.6. The external references of all relevant MySQL tests have been updated and mapped to the CIS MySQL 5.7 benchmark.

There are 40 new query-based tests that have been introduced in the 2018 Q4 DPS.

To download the CIS benchmark, use the following URL: https://www.cisecurity.org/cis-benchmarks/

### 2) VA scans with the latest STIG benchmark

Guardium 10.6 VA now supports STIG's latest DB2 10.5 benchmark version 1, release 1. For further information on the benchmark, see https://iase.disa.mil/stigs/app-security/database/Pages/index.aspx

You must execute the latest *gdmmonitor-db2.sql* script to run DB2 LUW VA as there are additional privilege requirements to execute these tests.

For more details, see Database privileges for Vulnerability Assessment.

There are 28 new query-based tests that have been introduced and already available as of the 2018 Q2 DPS. 3 new CAS tests are available for v10.6. The 10.6 CAS agent must be installed to utilize the new CAS tests.

**Query-based tests:**

| TEST_ID | TEST_DESC |
|---|---|
| 2621 | Access To External Executables Must Be Restricted |
| 2622 | Audit Policy CHECKING Category |
| 2623 | Audit Policy CONTEXT Category |
| 2624 | Is Audit Policy ERRORTYPE Set to A |
| 2625 | Audit Policy EXECUTE Category |
| 2626 | Audit Policy EXECUTEWITHDATA is Enabled |
| 2627 | Audit Policy OBJMAINT Category |
| 2628 | Audit Policy SECMAINT Category |
| 2629 | Audit Policy SYSADMIN Category |
| 2630 | Audit Policy VALIDATE Category |
| 2631 | Audit On System Catalog Authority objects |
| 2632 | CONNECT_PROC is Defined |
| 2633 | Audit Routine Execute Privileges |
| 2634 | Routine Ownership |
| 2635 | Package Ownership |
| 2636 | Module Ownership |
| 2637 | Trigger Ownership |
| 2638 | Tablespace Ownership |
| 2639 | Table Ownership |
| 2640 | Schema Authority |

| | |
|---|---|
| 2641 | Session Termination Threshold |
| 2642 | SSL_CIPHERSPECS is Defined |
| 2643 | SSL_SVR_LABEL is Defined |
| 2644 | SSL_VERSIONS is Defined |
| 2645 | Is Database Native Encryption enabled |
| 2646 | No Sample Database |
| 2647 | DB2 Communication Protocol SSL |
| 2648 | Password Encryption |

**CAS-based tests:**

| TEST_ID | TEST_DESC |
|---|---|
| 570 | Audit Data Path Permission |
| 571 | Log System Administrator Events |
| 572 | Log System Administrator Events - Windows |

### 3) DB2 z/OS Security APAR Test Enhancement:

Any APAR tests relevant to DB2 z/OS versions 8 & 9 have been deprecated. All APAR tests that aren't deprecated will now use a SIA number. Customers may use this information in the DB2 z/OS security portal to find the APAR ID, description and remediation details.

All short descriptions for the APAR tests will use the text "Possible security vulnerability in DB2 for z/OS".

All APAR tests will use the recommendation: "To fix SIA-DB2-2017.7-1 go to the IBM Z Security Portal, check the z/OS and z/VM SIA Cross-Reference record for Guardium APAR information and apply all outstanding fixes. If you aren't registered for access to the IBM Z Security Portal, please see https://www.ibm.com/it-infrastructure/z/capabilities/system-integrity"

### 4) Patch Test Enhancement:

If the database version and patch level are equal or higher than the defined levels, the security assessment passes. Previously, it required an exact match. For more information, see Modifying the database and patch level.

### 5) Oracle 18c

Guardium 10.6 supports the scanning of Oracle 18c on the Oracle cloud and on premise. CVE and patch test for Oracle 18c isn't supported.

## Known Issues and Workarounds

| Guardium Component | Bug # | Description |
|---|---|---|
| External S-TAP | GRD-21684 | If your site is deploying an External S-TAP to the Azure cloud (for a Microsoft Azure SQL database, make sure that the Azure SQL connection policy is set to “PROXY, rather than “REDIRECT” (the default). If set to REDIRECT, the External S-TAP can’t connect to SQL Server on Azure.<br><br>**Workaround:**<br><br>**Azure users:**<br>If your site is deploying an External S-TAP to the Azure cloud (for a Microsoft Azure SQL database, make sure that the Azure SQL connection policy is set to “PROXY, rather than “REDIRECT” (the default).<br><br>For information about how to change the connection policy, see the topic *Change Azure SQL Database Connection Policy* in the Microsoft Azure documentation. |
| External S-TAP | GRD-22655 | If the SSL_VERSION of Oracle client and Oracle server don’t match, an error can occur that will terminate the connection.<br><br>**Workaround:**<br><br>**Oracle users:**<br>Set both the Oracle client and server to TLS 1.2.<br><br>**Amazon RDS Oracle:**<br>To enable and set TLS for your database instance, add the SSL option to an Option Group, and apply the Option Group to your instance. Use the Oracle SSL “SQLNET.SSL_VERSION” option to specify the TLS version as one of the following: “1.0”, “1.2 or 1.0”, or “1.2”. The default SSL option is "1.0".<br><br>**For an Oracle on-premises instance:**<br><br>The TLS version is defined by the SSL_VERSION parameter in sqlnet.ora.<br><br>If you’re using the Oracle JDBC Driver to connect to the Oracle database, set the TLS version with the oracle.net.ssl_version JDBC connection property. The default is "any", so you’ll need to specify the exact version, for example, "TLS 1.2". |
| External S-TAP | GRD-24912 | External S-TAP When creating a certificate signing request (CSR), if the alias is longer than 20 characters the sniffer may not correctly transfer the CSR. |

| | | |
|---|---|---|
| | | **Workaround:** Use an alias that is less than 20 characters. |
| GIM | GRD-20542 | Windows GIM v10.5 requires reboot after uninstalling |
| Policy Builder | GRD-23030 | When a new session-level policy is installed from the Central Management page or Policy Builder for Data Page from a central manager on a managed unit, the GUI may display the sequence of installed policies incorrectly.<br><br>As an example, a newly installed session-level policy would be displayed as the last installed policy after existing data-level policies if install last option is chosen. However, the actual sequence in which the policies are applied isn't affected. Session-level policies are always installed and applied before data-level policies.<br><br>**Workaround:** To display the correct sequence in the GUI, install the policy from the Policy Builder for Data page from the managed unit. |
| Policy Builder | GRD-22989 | This issue is specific to an environment where the central manager is v10.6 but the managed units are of a lower version.<br><br>Policies affected:<br>1) Data set collection profile<br>2) Db2 collection profile<br>3) Db2 z/OS blocking profile<br>4) IMS collection profile.<br><br>When these policies are installed in two ways – either directly on a managed unit or by using the grdapi command 'grdapi install_policy', the installation will go through, but the policies won't work.<br><br>**There are two workarounds:**<br>**Solution 1:**<br>Apply Sniffer patch 4038 to managed units before installing these policies.<br><br>Download the Sniffer patch here: https://ibm.biz/BdY5zv<br><br>**Solution 2:**<br>Install the policies from the Policy Builder for Data page or Central Management page in the GUI. |
| Policy Builder | GRD-22555 | When importing policies from an earlier version of Guardium, the Criteria column of the Policy Rules panel may display settings that are inconsistent with the Rule Criteria panel settings for that rule. When this condition is present, the policy rules should behave as |

| | | |
|---|---|---|
| | | they did with the earlier version of Guardium when the policy was exported.<br><br>**Workaround:**<br>To correct the condition, edit the rule and set the affected criteria to its default value (or any appropriate value for the policy) and save the rule. After updating and saving the rule, the Criteria column of the Policy rules panel will match the Rule criteria panel settings. |
| Query- Report Builder | GRD-20831 | In the Build Expression dialog box that is used to create an expression for a query condition, "Save" doesn't work after clicking "Test". |
| CAS | GRD-20578 | Guardium Vulnerability Assessment CAS scripts for Sybase calls isql session with the -X option for initiating the login connection to the server with client-side password encryption. When the ASE environment settings aren't set or if they are incorrect, isql is unable to find the correct libraries and produces the error:<br><br>CT-LIBRARY error:<br>ct_connect(): protocol specific layer: internal Client Library error: There is a tds login error. The installed encryption handler returned a status that was not CS_SUCCEED.<br><br>**There are two workarounds:**<br><br>**Solution 1:**<br>Edit the SYBASE.sh file under the Sybase instance account.<br>Change:<br>SHLIB_PATH="/home/sybase16/DataAccess64/ODBC/lib:/home/sybase16/DataAccess64/ODBC/dm/lib64"<br>To:<br>SHLIB_PATH="/home/sybase16/DataAccess64/ODBC/lib:/home/sybase16/DataAccess64/ODBC/dm/lib64":$SHLIB_PATH<br><br>**Solution 2:**<br>Under the Sybase instance account, edit the .profile file to source both SYBASE.sh and SYBASE.env files. Make sure to source SYBASE.sh first, then SYBASE.env. |
| CAS | GRD-23308 | If CAS is installed using GIM without configuring the now optional parameter CAS_SQLGUARD_IP, an error occurs.<br><br>**Workaround:**<br>When using GIM to install CAS clients from a central manager, you must assign the client to a managed unit using the CAS_SQLGUARD_IP parameter. |

| | | |
|---|---|---|
| Sniffer | GRD-21438 | Defining a custom alert message subject line using the %%subject[] variable does not work with the default message template specified at Setup > Tools and Views > Global Profile.<br><br>**Workaround:**<br>To create an alert message with a custom subject line, use the %%subject[] variable in a named template. |
| REST API | GRD-17173 | This issue is specific to an environment where the central manager is v10.6 but the managed units are of a lower version.<br><br>On a site that uses Guardium REST APIs, the same client secret can't be used between upgraded central managers and older managed units.<br><br>**Workarounds:**<br><br>**Solution 1:**<br>Use client_secret directly from the central manager or register a new client for each managed unit that is connected to the central manager.<br><br>**Solution 2:**<br>Use the GuardAPI register_oauth_client CLI command.<br>Example: cli>grdapi register_oauth_client client_id=client_id1<br>For more information on this command, see Guardium REST API. |
| Health Analyzer | GRD-22939 | This issue is specific to the Health Analyzer running on a central manager or aggregator. The Analyzer doesn't identify or send alerts when sizes of databases or files on disk (/var) might potentially exceed the limit of 50 percent in the next 14 days. |
| Classifier | GRD-24473 | This issue is specific to a Guardium-generated GDPR discovery scenario.<br><br>When classification rules are filtered by a specific language using the language drop-down menu, the filter doesn't work as expected. As an example, when French is selected from the drop-down menu, the classification rules appear to be filtered. However, when you run the scenario, the results aren't filtered.<br><br>**Workaround:**<br><br>To filter by a specific language, follow these steps:<br><br>1. In the Discover Sensitive Data page, delete all existing rules from the "Selected Classification Rules" section.<br>2. Use the filter in the "Classification Rule Templates" section to filter rules for a specific language<br>3. Move the filtered rules to the Selected Classification Rules table |

| | | |
|---|---|---|
| | | 4. Repeat for each language, as needed |
| Audit Process Builder | GRD-14726 | This issue is specific to the task types: Report, Privacy Set and Entity Audit Trail. It occurs in a scenario where more than one task is defined in the audit process.<br><br>In the task parameters section of a new task, the "off" option of the show aliases radio button (SHOW_ALIASES) doesn't work as expected.<br><br>As an example, when you run a report with Aliases turned off, the results are displayed for aliases rather than original values.<br><br>**Workaround:**<br>On the results page, use the radio buttons "Show Original Values" or "Use Aliases" to filter results as needed. |
| Backup and restore | GRD-24450 | When backup restore process is completed using the CLI command background `restore db-from-prev-version`, you must manually restore both the current appliance IP and System Host Name using the CLI commands: `store network interface ip <x.x.x.x>` and `store system hostname <hostname>` |
| Data Protection Dashboard | GRD-23085 | The drag and drop feature on the Guardium Data Protection Dashboard only allows dragging to the right.<br><br>**Workaround:** instead of dragging to left, drag to right so that the right-hand graph shifts to the left. |
| Investigation Dashboard | GRD-22513 | Investigation dashboard doesn't work on IE 11.<br><br>**Workaround:** open the Investigation dashboard in a supported browser. |
| External Feed/System | GRD-20797 | When running high-load concurrent processes, there's a race condition where date and time fields could be incorrectly updated.<br><br>**Workaround:** This is a rare condition. Until the fix is introduced, customers who experience this issue can avoid running these processes concurrently: external feeds, reports, audit processes. This will be fixed in post 10.6 bundles. |
| UNIX S-TAP | GRD-19047 | When running the OS command nzrestore with Log Full Details Guardium policy action on the user only logs session start and end. This is because Netezza DB doesn't support IPC traffic.<br><br>**Workaround:** Add another IE with PGSQL as db-type and intercept_type=npipe. For example, if Netezza IE is:<br>[DB_1]<br>connect_to_ip=127.0.0.1 |

| | | |
|---|---|---|
| | | db2_fix_pack_adjustment=20<br>db2_shmem_client_position=0<br>db2_shmem_size=131072<br>db2bp_path=NULL<br>db_exec_file=/nz/kit.7.2.1.0/sbin/postmaster<br>db_install_dir=/export/home/nz<br>db_type=PGSQL<br>encryption=0<br>db_version=7<br>instance_running=1<br>intercept_types=npipe<br>load_balanced=1<br>port_range_end=5480<br>port_range_start=5480<br>priority_count=20<br>real_db_port=5480<br>tap_identifier=netezza_72nzsimbeta(5480,5480,DB_0)<br>tee_listen_port=0<br>unix_domain_socket_marker=NULL<br>networks=0.0.0.0/0.0.0.0<br>exclude_networks=<br>Copy the existing IE, change DB_TYPE=PGSQL, and intercept_types=npipe. |
| Ecosystem | GRD-22486 | Due to third-party library updates, Ecosystem applications previously installed on a v10.5 Guardium appliance will be incompatible with v10.6 when upgrading to GPU 600, resulting in the applications being permanently disabled.<br><br>Applications previously installed on v10.5 must be reinstalled after installing GPU 600. Note: Application data won't be preserved.<br><br>The installation of new applications on a v10.6 Guardium appliance isn't affected. |
| Solr | GRD-24444 | Quick Search may not work after switching from a Central Manager to a Backup Central Manager.<br><br>**Workaround:**<br>Restart the GUI on the Central Manager first. After it's up, restart it on all the Managed Units. Once this is done, the search data from before switch becomes visible and new data is indexed. |

## Changes in API Behavior

This section reflects changes in API behavior from previous Guardium releases.

| Changes in API/Entity | Description of changed behavior |
|---|---|
| gim_uninstall_module<br><br>**Older Guardium versions:**<br>REST_VERB: GET<br><br>**Update in 10.6:**<br>REST_VERB: DELETE | The REST verb for the API gim_uninstall_module has changed from GET to DELETE. Any code that uses this API function must be modified to the new REST verb. |
| GIM Modules Heartbits<br><br>**Older Guardium versions:**<br>entity = GIM Modules Heartbits<br>table = GIM_MODULES_HEARTBITS<br><br>**Update in 10.6:**<br>entity = GIM Modules Heartbeats<br>table = GIM_MODULES_HEARTBITS | When using Guardium APIs to reference the entity label "GIM Modules Heartbeats, use the table name GIM_MODULES_HEARTBITS.<br><br>For example:<br>grdapi create_computed_attribute attributeLabel="Module Status" entityLabel="GIM Modules Heartbeats" expression= "IF(GIM_MODULES_HEARTBITS.GIM_LAST_UPDATE>date_add(CURRENT_TIMESTAMP,INTERVAL -1 HOUR),'UP','DOWN')" |
| **Older Guardium Versions:**<br>grdapi set_classification_concurrency_limit<br>grdapi get_classification_concurrency_limit<br><br>**Update in 10.6:**<br>grdapi set_job_process_concurrency_limit<br>grdapi get_job_process_concurrency_limit | The Vulnerability Assessment multi-threading feature now supports both classification and assessment.<br><br>The new Guardium API command "set_job_process_concurrency_limit" defines the number of assessment *and* classifier processes that can run concurrently. |

## Bug Fixes

| Issue Key | Summary | APAR |
|---|---|---|
| GRD-7686 | Follow up RTC 41180 SAP app user name truncation | |
| GRD-10355 | GIM install should not change permissions on /etc/inittab | GA16382 |
| GRD-11080 | Trusted Apps not always showing with Ignore STAP Session | GA16507 |
| GRD-13332 | Guardium agents doesn't start after the server gets rebooted | GA16452 |
| GRD-13821 | KRB_* parameters should not be set | GA16566 |
| GRD-14803 | must gather system_output.txt misleading - "Output of Checking Total Memory" - and states "Total RAM Memory of the appliance" is "in the required range" when it isn't | GA16531 |
| GRD-15270 | Possible Security problem - http status 403 - use a risk analysis tool - change the HTML "Get" Method function to "Options" Method - can be used by attacker | GA16530 |
| GRD-15507 | New GIM "Setup up by Client" application does not allow Cancell Uninstall button to clear "failed installation" status | GA16534 |
| GRD-15676 | Questionable (wrong) join in Analytics domain between entitles: analytic outlier and analytic outlier | GA16476 |
| GRD-15677 | Export csv in investigation dashboard functionality | GA16474 |
| GRD-15679 | Enterprise Load balancer doesn't relocate STAPs, that have more than one Sqlguard IP. | GA16580 |
| GRD-15786 | snif.log 1000s messages (related to STAP LB) that monitors snif liveliness by opening a connection (and then closing it) | |
| GRD-15969 | email send not working | GA16486 |
| GRD-16070 | Only the admin user can see VA Test domains | GA16601 |
| GRD-16077 | equifax_secure_certificate_authority cert expires on all appliances in 6 months( ie. Aug 22) | GA16426 |
| GRD-16096 | Unable to add MySQL IE after Win STAP upgrade to 10.2.40.68 (collector is 10.1.2) | GA16597 |
| GRD-16105 | Request Timeout Params for Hung Datasources during Custom table data upload | GA16575 |
| GRD-16322 | STAP_r102728 suspected of causing kernel panic | GA16355 |
| GRD-16356 | Amazon S3 configuration not saving for data archive nor system backup | Doc Update |
| GRD-16460 | Time Period data from customers is distributed to all customers | GA16328 |
| GRD-16524 | Guardium Appliances are running at TSM Client Level 7.1.6.2 | GA16468 |
| GRD-16631 | The function create_member_to_group_by_desc don't handle "registered trademark symbol (R)" or "copyright symbol (c)" | GA16332 |
| GRD-16794 | Some of Windows S-TAP must gather files are missing when trying to get them from GUI | |
| GRD-16840 | 10.1.4 \|\| REST enable test_datasource_connection | GA16365 |
| GRD-17039 | Guardium and GreenplumDB for versions 4.3.8.1 and 4.3.22.1 | GA16470 |
| GRD-17241 | Aggregation Performance Issue | GA16522 |

| | | |
|---|---|---|
| GRD-17247 | Scheduled Job DREP stuck in IN_TRANST or ERROR state due to SCP error | GA16565 |
| GRD-17316 | cleanup_oldfiles.sh via cron fails because of an incorrect FIND command | GA16501 |
| GRD-17455 | Multiple gim_xxx.conf files in /etc/init will not allow GIM to start | |
| GRD-17573 | 10.1.4 \|\| Group Builder (Legacy) \|\| Group Member Addition Inconsistency ["DIP"] instead of ["DIP"]. | GA16520 |
| GRD-17630 | I would want a CLI command to set MaxMessageSize to whatever in rsyslog.conf | GA16536 |
| GRD-17679 | Post Installing VMWARE_TOOLS, the services on appliance did not start automatically | GA16521 |
| GRD-17703 | system messages not being written to syslog | GA16559 |
| GRD-17785 | STAP is somehow slowing down Batch and ETL jobs in Teradata environment | GA16589 |
| GRD-17805 | Cannot reset accessmgr password using <N> in 10.1.4 | GA16368 |
| GRD-17843 | DB Name is Null when login failed in MSSQL 2014(with V9 WINSTAP) | GA16374 |
| GRD-17865 | Guardium v10.1.4 STAP/KTAP Logs Filling DB Root Partition | GA16489 |
| GRD-17886 | (Enhancement) Zip diagnostic files before sending to the collector | |
| GRD-17910 | CORRELATION_TIMEOUT parameter can't be seen in grdapi | |
| GRD-17912 | User Audit trail doesn't reflect changes to ACCESS_RULE_ACTION entity | GA16358 |
| GRD-17919 | grdapi add_assessment_test failing because of comma in predefined test name | GA16592 |
| GRD-17920 | VA grdapi update_assessment_test should allow update to the "exceptionsGroup" | GA16591 |
| GRD-17925 | Guardium STAP/KTAP Logs Filling DB Root Partition | GA16564 |
| GRD-17975 | Import failed \|\| Error: Day cannot be imported twice | GA16621 |
| GRD-18045 | Problems importing from external datasource via group builder | GA16582 |
| GRD-18203 | STAPs point to collector as Enterprise Load balancer | GA16579 |
| GRD-18213 | Guardium STAP using high CPU | GA16587 |
| GRD-18215 | STAP_r102728 suspected of causing kernel panic | GA16478 |
| GRD-18226 | Table optimization fails | GA16490 |
| GRD-18301 | Aliases in audit report result in GUI and the export of the same audit report result in PDF, or CSV file does not match. | GA16446 |
| GRD-18364 | SQL comments that can execute hidden selects etc isn’t logged for MySQL and mariadb | GA16370 |
| GRD-18395 | 3-digit octal number (#012 #011) in syslog after upgrading to p400 | GA16360 |
| GRD-18408 | DB2 Exit seems to append chars to DB User | GA16453 |
| GRD-18490 | Remove tls-decrypt cli commands | GA16485 |
| GRD-18611 | STAP crash : ANOM_ABEND comm="guard_stap" reason="memory violation" sig=11 | GA16505 |
| GRD-18616 | 7 tuple isn’t available in client server entity through custom domain | GA16372 |

| | | |
|---|---|---|
| GRD-18676 | How to install custom CAS certificate | GA16386 |
| GRD-18894 | Vulnerability Assessment test giving false negatives | GA16469 |
| GRD-19002 | Group name is replaced with GROUP_ID after clone with "NOT LIKE GROUP" | GA16600 |
| GRD-19135 | Reason For Huge Traces of "ERROR: process_krb_token() tobuf_len is 0" from STAP | GA16422 |
| GRD-19169 | Request was interrupted or quota exceeded | GA16537 |
| GRD-19195 | V10.1.4 \|\| MongoDB 3.6.5 \|\| A-TAP Activation & Encrypted Traffic Issue | GA16451 |
| GRD-19196 | Details attribute is cut in predefined Classification Process Log report | GA16224 |
| GRD-19296 | VA Test for SYBASE IQ, Locked accounts, is throwing an Error even when on SYBASE IQ 16.0 | GA16573 |
| GRD-19460 | grdapi command fails with Err=2410 for the used expression | GA16558 |
| GRD-19509 | Using full hostname when installing bundle STAP not working | GA16514 |
| GRD-19640 | Sybase IQ setup with ATAP may become unresponcive or even crash | GA16547 |
| GRD-19671 | System CPU% and System Idle CPU% are 0% in the UNIX STAP Statistics report | GA16380 |
| GRD-19719 | Improve removing red STAPS from original MU in Enterprise Load Balancer environment to get rid of false red staps | |
| GRD-19791 | GIM fails to install because of tapip issue | GA16473 |
| GRD-19851 | Auditprocess entry with new tomcat process id added | GA16479 |
| GRD-19902 | Audit process aliasing isn't shown in the syslog | GA16481 |
| GRD-19993 | V10.5 \|\| ALERT BUILDER \|\| "Message Template" and "Central Manager" modification changes do not get retained | GA16390 |
| GRD-20048 | Custom Upload of GDM_STATISTICS pulls the wrong hours. | GA16571 |
| GRD-20081 | Scheduled Tomcat restart does not honor schedule | GA16496 |
| GRD-20095 | Does Guardium support 'store network dhcp' on VMware ESX Server? | GA16403 |
| GRD-20097 | query about ktap_fsmon_buffer_size parameter | GA16393 |
| GRD-20102 | Computed attribute content isn't properly displayed in Guardium | GA16542 |
| GRD-20228 | Data Protection Dashboard, unable to drop visualizations on Firefox & Chrome | GA16483 |
| GRD-20313 | Built-in report "Installed Policy Details" fails to run as an Audit task | GA16500 |
| GRD-20424 | Outer Join isn't properly handled within custom domain functionality | GA16215 |
| GRD-20443 | grdapi will not add members to a group if the name has a + in it | GA16440 |
| GRD-20476 | stap upgrade fails for UNIX dbservers when STAP_TAP_IP is hostname | GA16471 |
| GRD-20507 | User cannot view audit process results when a report is used. Same role CAN see results if Security Assessment is used | GA16602 |
| GRD-20615 | installdir and port isn't correct after installation of stap. | GA16535 |

| | | |
|---|---|---|
| GRD-20622 | Classification policy created by grdapi not working \|\| GPU 500 | GA16509 |
| GRD-20653 | Audit Process Report gets completed but not able to download results as PDF | GA16524 |
| GRD-20654 | Instance discovery creating incorrect IE for Oracle | GA16448 |
| GRD-20673 | guard_diag does not contain guard_discovery.stderr.log | GA16484 |
| GRD-20810 | Sometimes ADMINCONSOLE.txt in mustgather does not contain data | GA16590 |
| GRD-20909 | Audit Process Builder "Schedule by Month" options merged into one on v10.1.4 and v10.1.5 - Japanese only | GA16429 |
| GRD-20925 | Aggregation/Archive Log Details cannot be viewed even when role grants the Errors Report accessible | GA16513 |
| GRD-20969 | Reporting issues custom query result count less than collector | GA16554 |
| GRD-21215 | The "export file" cli command is unable to process must_gather files, failing with error "ERROR: No exporting of system files." | GA16435 |
| GRD-21366 | INCONSISTENT SERVER_HOSTNAME in GDM_ACCESS. Column Cannot be used in reports | GA16427 |
| GRD-21401 | Duplicate entry error on inserting to GDM_SESSION_LIVE | GA16433 |
| GRD-21539 | Core Dump errors generated over AIX Server, v10.1.4 | GA16447 |
| GRD-21598 | Java heap space issue for audit process with large result set | GA16482 |
| GRD-21855 | S-Tap causing server crash | GA16447 |
| GRD-22094 | Aggregation/Archive Errors alert will alert on an informational message | |
| GRD-22174 | S-TAP Info (STAP_INFO) Custom Table's Purge is set to the default (0 months) after patching (P4035 / P505). | GA16523 |
| GRD-22257 | STAP beta version for Cassandra Encrypted Compressed Traffic | GA16506 |
| GRD-22462 | VA \|\| MS SQL Server \|\| "DDL granted to user" | GA16519 |
| GRD-22481 | Session Start / Session End (maybe others) are missing in list of main entities in access domain | |
| GRD-22524 | Persistent Cross-Site Scripting (XSS) User login request issue PSIRT 123872 | GA16529 |
| GRD-22553 | Need to monitor usage of soft limits | GA16562 |
| GRD-22606 | System Shared Secret and Clear text password isn’t encrypted in GUARD_USER_ACTIVITY_AUDIT | |
| GRD-22667 | RestAPI gim_uninstall_module command record contains incorrect REST_VERB | GA16487 |
| GRD-22707 | Group Builder doesn't treat Qualified Object properly | GA16488 |
| GRD-22976 | Cannot connect to DB after ATAP configuration | GA16494 |
| GRD-23023 | Discrepancy between audit jobs on CM and child aggs | |
| GRD-24901 | External S-TAP: Cannot connect to collector with S-TAP Certification enabled | |

## Security Fixes

| Issue Key | PSIRT ID | CVEs | Description |
|---|---|---|---|
| GRD-12880 | 104194 | CVE-2011-5320 CVE-2017-15670 CVE-2017-15671 CVE-2017-15804 | Using components with Known Vulnerabilities (GNU glibc) |
| GRD-13967 | 121593 | CVE-2015-5237 CVE-2017-3162 CVE-2017-3161 CVE-2017-15713 CVE-2016-6811 CVE-2016-5001 CVE-2014-3627 CVE-2014-0229 | Using Components with Known Vulnerabilities (hadoop-auth) |
| GRD-16260 | 101242 | CVE-2017-1597 | GUI user password compliance |
| GRD-16651 | 115679 | CVE-2018-8012 | Using Components with Known Vulnerabilities (Zookeeper) |
| GRD-17173 | 113327 | CVE-2018-1498 | Password in clear text vulnerability |
| GRD-17187 | 113378 | CVE-2015-3254 | Using components with Known Vulnerabilities (libthrift) |
| GRD-17205 | 113379 | CVE-2015-3254 | Using components with Known Vulnerabilities (libfb) |
| GRD-17206 | 113382 | CVE-2018-1509 | Improper Certificate Validation Vulnerability |
| GRD-17945 | No PSIRT ID | CVE-2017-3145 | Using Components with Known Vulnerabilities (BIND) |
| GRD-17946 | 121640 | CVE-2018-5733, CVE-2018-5732 | Using Components with Known Vulnerabilities (DHCP) |
| GRD-17948 | 121637 | CVE-2017-5715 | Using Components with Known Vulnerabilities (microcode_ctl) |
| GRD-20803 | 121263 | CVE-2018-1817 | Cross-Site scripting Vulnerabilities |
| GRD-20821 | 121633 | CVE-2018-1284 CVE-2018-1282 CVE-2016-3083 | Using Components with Known Vulnerabilities (Hive-exec) |

| | | | |
|---|---|---|---|
| GRD-20822 | 121635 | CVE-2018-1000156 | Using Components with Known Vulnerabilities (patch) |
| GRD-20847 | 121264 | CVE-2018-1818 | Use of Hard-coded Credentials Vulnerability |
| GRD-20891 | 120981 | CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2018-1000156, CVE-2018-8897, CVE-2017-1000410, CVE-2017-13166, CVE-2017-7645. CVE-2017-8824. CVE-2017-18017, CVE-2018-3639, CVE-2018-1124, CVE-2018-1126, CVE-2017-8890, CVE-2018-3639, CVE-2018-1130, CVE-2017-18203, CVE-2017-15121, CVE-2017-12190, CVE-2017-9077, CVE-2017-9076, CVE-2017-9075, CVE-2018-5803, CVE-2017-7616, CVE-2017-7308, CVE-2017-6001, CVE-2017-2671, CVE-2016-8650, CVE-2015-8830, CVE-2012-6701, CVE-2017-7889, CVE-2018-3665, CVE-2018-3639, CVE-2018-10675, CVE-2018-1000004, CVE-2018-7566, CVE-2018-3693. CVE-2018-3646. CVE-2018-3620. CVE-2017-15265. CVE-2017-0861. CVE-2018-10901 | Using components with Known Vulnerabilities (kernel) |
| GRD-21709 | 121638 | CVE-2018-1126 CVE-2018-1124 | Using Components with Known Vulnerabilities (procps) |
| GRD-22524 | 123872 | CVE-2018-1889 | Cross-Site scripting Vulnerabilities |
| GRD-22645 | 123879 | CVE-2018-1891 | Cross-Site scripting Vulnerabilities |
| GRD-2468 | 91258 | CVE-2016-1181 CVE-2016-1182 | Using components with Known Vulnerabilities (Apache Struts) |
| GRD-4187 | 93726 | CVE-2017-1268 | GUI user password strengthening |
| GRD-4448 | 93730 | CVE-2017-1272 | Query Parameter in SSL requests Vulnerability |
| GRD-6202 | 93723 | CVE-2017-1265 | Improper Certificate Validation Vulnerability |

| | | | |
|---|---|---|---|
| GRD-7630 | 91252 | CVE-2015-0899 | Using components with Known Vulnerabilities (Apache Struts) |
| GRD-7630 | 98818 | CVE-2016-3092 CVE-2014-0114 | Using components with Known Vulnerabilities (Apache Struts) |
| GRD-8563 | 121634 | CVE-2017-15670 CVE-2017-15804 | Using Components with Known Vulnerabilities (glibc) |
| GRD-9934 | 101242 | CVE-2017-1597 | GUI user password strengthening |

## Releases for v10.0 since v10.5

| Patch# | Bug # | APAR | Description |
|---|---|---|---|
| V10.0p505 | | | Link to release notes: https://delivery04.dhe.ibm.com/sar/CMA/IMA/07obe/0/Guardium_v10_0_p505_Bundle_release_notes.pdf |
| V10.0p508 | GRD-19051 | | Fix Instance of Alert Builder does not allow creating a custom threshold |
| V10.0p509 | GRD-18890 | | Guardium Data Set Collection Profile Policy hitting group limit of 1488 |
| V10.0p510 | GRD-20845 | | Alerter Fixes:<br>• Fixed instance of Alerter sending one message per polling interval<br>• Fixed instance of Alerter marking messages as FAIL in error<br>• Fixed instance of Alerter performance issues due to an extra mysql query |
| V10.0p512 | GRD-13356 | | A manual snmpd restart is required to obtain extOutput.2 metric successfully post appliance reboot |
| | GRD-14415 | | 10.1.4 Classifier job halts after 1-2 hours |
| | GRD-16077 | GA16426 | equifax_secure_certificate_authority cert expires on appliances on Aug 22 |
| | GRD-17094 | | Classification scan with Netezza data sample size of 2000 and sample type Random issue |
| | GRD-17563 | GA16431 | Security Assessment DataSource for MongoDB replica sets should auto detect primary instance. |
| | GRD-17753 | GA16356 | Mysql Disk Usage shows different value on GUI and CLI |
| | GRD-18301 | GA16446 | Aliases in audit report result in GUI and the export of the same audit report result in PDF, or CSV file does not match. |
| | GRD-18622 | | TTY respawn syslog messages still shows up in syslog even after "store system serialtty off" |
| | GRD-18824 | GA16444 | Schedule Job Exception: The current column selected for the query is no longer valid. |
| | GRD-19096 | | Custom template isn’t stored in alert builder |

| Patch# | Bug # | APAR | Description |
|---|---|---|---|
| | GRD-19441 | GA16376 | System Backup fail - 'ERROR: Backup file was not copied. Method=SCP' |
| | GRD-19460 | | grdapi command fails with Err=2410 for the used expression |
| | GRD-19993 | GA16390 | ALERT BUILDER: "Message Template" and "Central Manager" modification changes do not get retained |
| | GRD-20424 | | Outer Join isn't properly handled within custom domain functionality |
| | GRD-20443 | GA16440 | grdapi will not add members to a group if the name has a + in it |
| V10.0p513 | GRD-22118 | | v10p512 fails to authenticate when LDAPS is used to authenticate users |
| V10.0p514 | GRD-21538 | GA16456 | Classifier data scan does not match Netezza tables |
| V10.0p515 | GRD-21798 | | Incident generation isn't generating the INCIDENT sometimes |
| V10.0p516 | GRD-13921 | | AMI Support |

## Sniffer Updates since v10.5

Latest sniffer patch included in GPU 600: v10.0 patch 4040

Notes:

Installation of sniffer patches must be scheduled during a "quiet" time on the Guardium appliance to avoid conflicts with other long-running processes (such as heavy reports, audit processes, backups, imports and so on).

Installation of sniffer patches will automatically restart the sniffer process.

If the downloaded package is in .zip format, customers are required to unzip it outside the Guardium appliance before installation.

Universal sniffer patch can be installed on top of any GPU starting with v10.0 patch 100 or higher.

If there's a failure to install, the following error message will display:
ERROR: Patch Installation Failed - Incompatible GPU level. GPU p100 or higher required.

This sniffer patch should be installed across all the appliances: central manager, aggregators and collectors to avoid aggregator merge issues.

**Important:** Any superseding sniffer or security patches must be reinstalled after installing GPU 600.

| Sniffer Update | Bug# | APAR | Description |
|---|---|---|---|
| 4033 | | | Link to patch 4033: https://delivery04.dhe.ibm.com/sar/CMA/IMA/07kr3/0/Guardium_v10_0_p4033_sniffer_update_release_notes.pdf |
| | GRD-12713 | | Sniffer change to address quotes in objects generate duplication in reporting |
| | GRD-15806 | GA16307 | p4030 does not record RESPONSE_TIME |
| | GRD-16047 | GA16508 | Sniffer Restarts due to being killed by SEGV Signal on Sniffer p4030 |
| | GRD-16355 | GA16353 | v10 Guardium report incorrectly shows Full_SQL.Succeeded=1 for the first SQL statement in a batch of SQL that all fail - for MSSQL SERVER MANAGEMENT STUDIO |
| | GRD-16396 | GA16352 | Double Quotes within DB User cause policy not to match |
| | GRD-16918 | GA16533 | "Records Affected -1" for Oracle WITH clause |
| | GRD-16924 | GA16518 | Siebel Application User Translation not working as expected. |

| | | | |
|---|---|---|---|
| | GRD-17585 | PI97785 | SQL Alter Procedures Not Captured after v10.1.4 Snif 4031 installation on UDB Server |
| 4034 | GRD-17456 | | Implement masking of sensitive data in exceptions by pattern - sent to alert |
| | GRD-17861 | GA16414 | Fix Different CEF Behavior for Alert Per Match and Alert Only |
| | GRD-14377 | | Implement masking of sensitive data in exceptions by pattern |
| 4035 | GRD-13703 | GA16292 | Alert CEF template variable values need to escape backslash |
| | GRD-15737 | GA16539 | Large number of Netezza parser errors in GDM_ERROR table resulting in DB full |
| | GRD-17312 | GA16384 | Login failed exceptions not captured with selective audit policy on p4029 |
| | GRD-17755 | GA16400 | Collector not logging the PostgreSql "ALTER SYSTEM" command \|\| SUP-4031 |
| | GRD-17910 | | CORRELATION_TIMEOUT parameter can't be seen in grdapi |
| 4036 | GRD-17786 | | Incorrect mapping of Cloudera events to Guardium fields |
| 4037 | GRD-20312 | GA16516 | Excessive rows generated on GDM_FIELDs |
| | GRD-20304 | GA16511 | Cassandra 3.11 database session traffic causing sniffer crash issue |
| | GRD-20083 | GA16401 | object for the DROP TRIGGER sql for MSSQL is not parsed |
| | GRD-12206 | GA16407 | Mongodb with sniffer p4029 db_user = NO_AUTH |
| 4038 | GRD-13779 | GA16394 | Capture Netezza session information |
| | GRD-16972 | GA16598 | Sniffer crashing "stuck condition = timestamp" |
| | GRD-19094 | GA16437 | SQL Server Create Function logs two statements rather than a single statement |
| | GRD-19566 | GA16599 | Netezza GRANT statements showing in GDM_ERROR |
| | GRD-19571 | GA16450 | Grant statements not being logged by Guardium in Oracle multitenant environment |
| | GRD-20130 | GA16512 | No traffic from KAFKA for Cloudera Hadoop |
| | GRD-20835 | GA16449 | Query rewrite of a column isn’t working if you got convert statement before it |
| | GRD-21401 | GA16433 | Duplicate entry error on inserting to GDM_SESSION_LIVE |
| 4039 | GRD-20130 | GA16512 | Additional improvements for capturing traffic from KAFKA for Cloudera Hadoop |
| 4040 | GRD-23277 | | CouchDB shows that DB_USER has changed to the wrong value. |

## New Platforms and Databases supported in v10.6

### New Support for UNIX S-TAP

**Platforms**
Ubuntu 18

**Databases**
PostgreSQL 9.6
PostgreSQL 10
Oracle 18
MongoDB 4
Teradata 16.1
Teradata 16.2
Cloudera 5.12
Hortonworks 2.6
SAP HANA V2 SPS02
Aster DB 6.2 (no encryption support)
Greenplum 5.7

### New Support for Windows S-TAP

**Databases**
MongoDB 4
MSSQL 2017
Oracle 18
PostgreSQL 9.6
PostgreSQL 10

## Deprecated Functionality

Legacy query builder and report builder are replaced by new query-report builder.

Classification policy builder and classification process builder are deprecated and replaced by discover sensitive data scenario.

Baseline, AME, windows file monitor, capture/replay and access map.

## Additional Resources

**IBM Security Guardium Knowledge Center and online help**
http://www-01.ibm.com/support/knowledgecenter/SSMPHH/SSMPHH_welcome.html

**REST API and GuardAPI reference**
Guardium API A-Z Reference

**System Requirements and Supported Platforms v10.6**
https://www-01.ibm.com/support/docview.wss?uid=ibm10719695

**Software Appliance Technical Requirements v10.6**
https://www-01.ibm.com/support/docview.wss?uid=ibm10744773

**IBM Security Learning Academy**
See securitylearningacademy.com for learning more about Guardium.

**Flashes and Alerts for IBM Security Guardium**
https://ibm.biz/BdY5fe

2018-December-11